

**UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
GREENBELT DIVISION**

PATI SPRINGMEYER, an individual and
Nevada Resident, on behalf of herself and all
others similarly situated,

Plaintiff,

v.

MARRIOTT INTERNATIONAL, INC., a
Montgomery County, Maryland Resident,

Defendant.

CASE NO.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

- (1) Negligence
- (2) Negligence *Per Se*
- (3) Breach of Contract
- (4) Breach of Implied Contract
- (5) Breach of Confidence
- (6) Deceptive & Unfair Trade Practices

For her Class Action Complaint, Plaintiff Pati Springmeyer, on behalf of herself and all others similarly situated, allege the following against Defendant Marriott International, Inc. (“Marriott”), based on personal knowledge as to herself and on information and belief as to all other matters based upon, *inter alia*, the investigation conducted by and through Plaintiff’s counsel:

SUMMARY OF THE CASE

1. Marriott is one of the largest hotel chains in the world servicing tens of millions of customers every year.

2. As part of the reservation and booking process for staying at a Marriott property, Marriott’s guests create, maintain, and update profiles containing significant amounts of personal identifiable information (“PII”), including their names, birthdates, addresses, locations, email addresses, and payment card information.

3. On March 31, 2020, Marriott announced that the login credentials of two of its employees had been compromised and “an unexpected amount of guest information” had been

improperly accessed as early as mid-January 2020. The compromised guest PII included: Contact Details (e.g., name, mailing address, email address, and phone number); Loyalty Account Information (e.g., account number and points balance, but not passwords); Additional Personal Details (e.g., company, gender, and birthday day and month); Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers); and Preferences (e.g., stay/room preferences and language preference) (“Data Breach”).

4. This Data Breach comes on the heels of another massive breach Marriott announced in November 2018, wherein the PII of 500 million guests contained in Marriott’s Starwood reservation database was exposed due to a flaw in its reservation and database systems.

5. This Data Breach was a direct result of Marriott’s failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its guests’ PII.

6. Marriott disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard guest PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiff and Class Members with prompt and accurate notice of the Data Breach.

7. As a result of Marriott’s failure to implement and follow basic security procedures, guest PII is now in the hands of thieves. Plaintiff and Class Members have had to spend, and will continue to spend, significant amounts of time and money in an effort to protect themselves from the adverse ramifications of the Data Breach, and will forever be at a heightened risk of identity theft and fraud.

8. Plaintiff, on behalf of all others similarly situated, allege claims for negligence, breach of confidence, and violation of the Maryland's Consumer Protection Act, and seek to compel Defendant to adopt reasonably sufficient security practices to safeguard guest PII that remains in its custody in order to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendant and is a citizen of a foreign state. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

10. Venue is proper under 28 U.S.C. § 1391(c) because Defendant is a corporation that does business in and is subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including the decisions made by Marriott's governance and management personnel that led to the breach. Further, Marriott's terms of service governing users in the United States provides for Maryland venue for all claims arising out of Plaintiff's relationship with Marriott.

PARTIES

11. Plaintiff Pati Springmeyer is a resident and citizen of Las Vegas, Nevada. Plaintiff Springmeyer has stayed at a number of Marriott properties and hotels over the past 10 years, entrusting Marriott with her PII. On March 31, 2020, Ms. Springmeyer received an email from

Marriott International stating that her PII had been compromised and “accessed without authorization.”

12. Since the announcement of the Data Breach, Ms. Springmeyer continues to monitor her various accounts in an effort to detect and prevent any misuses of her personal information.

13. Ms. Springmeyer has, and continues to spend her valuable time to protect the integrity of her PII — time which she would not have had to expend but for the Data Breach.

14. Ms. Springmeyer suffered actual injury from having her PII exposed as a result of the Data Breach including, but not limited to: (a) paying monies to Marriott for its services which she would not have, had Marriott disclosed that it lacked data security practices adequate to safeguard consumers’ PII from theft; (b) damages to and diminution in the value of her PII—a form of intangible property that the Plaintiff entrusted to Marriott as a condition for hotel services; (c) imminent and impending injury arising from the increased risk of fraud and identity theft.

15. As a result of the Data Breach, Ms. Springmeyer will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come.

16. Defendant Marriott, Inc., is a corporation with its principal executive offices located at 10400 Fernwood Rd, Bethesda, Maryland 20817.

FACTUAL BACKGROUND

A. The Marriott 2020 Data Breach

17. In February 2020, Marriott learned that the login credentials of two employees at a franchise property had been compromised a large amount of guest PII had been improperly accessed. Over a month later, Marriott notified approximately 5.2 million guests that their PII such as names, addresses, phone numbers, birthdays, loyalty information had been compromised. Although Marriott said it doesn’t believe that credit card information, passport numbers or driver’s

license information were accessed, they stated the investigation was ongoing and they did not rule out the possibility.¹

18. On March 31, 2020, Marriott sent an email to affected guests and posted an incident notification on its website stating in relevant part as follows:

Marriott International: Incident Notification

This site has information concerning the incident, answers to questions, and steps guests can take.

March 31, 2020

What Happened?

Hotels operated and franchised under Marriott's brands use an application to help provide services to guests at hotels. At the end of February 2020, we identified that an unexpected amount of guest information may have been accessed using the login credentials of two employees at a franchise property. We believe this activity started in mid-January 2020. Upon discovery, we confirmed that the login credentials were disabled, immediately began an investigation, implemented heightened monitoring, and arranged resources to inform and assist guests.

Although our investigation is ongoing, we currently have no reason to believe that the information involved included Marriott Bonvoy account passwords or PINs, payment card information, passport information, national IDs, or driver's license numbers.

At this point, we believe that the following information may have been involved, although not all of this information was present for every guest involved:

- Contact Details (e.g., name, mailing address, email address, and phone number)
- Loyalty Account Information (e.g., account number and points balance, but not passwords)

¹ *Millions of Guests Impacted in Marriott Data Breach, Again*, Threatpost, March 31, 2020, <https://threatpost.com/millions-guests-marriott-data-breach-again/154300/>

- Additional Personal Details (e.g., company, gender, and birthday day and month)
- Partnerships and Affiliations (e.g., linked airline loyalty programs and numbers)
- Preferences (e.g., stay/room preferences and language preference)

Guest Notification

On March 31, 2020, Marriott sent emails about the incident to guests involved. The email was sent from marriott@email-marriott.com because this is the standard email account used to communicate with our guests.²

B. Marriott Acquires, Collects, and Stores Plaintiff's and Class Members' PII

19. Marriott is an American multinational, diversified hospitality company that manages and franchises a broad portfolio of hotels and related lodging facilities, including 30 brands with more than 7,000 properties across 130 countries and territories globally. Founded in 1927, the company is headquartered in Bethesda, Maryland, and maintains hotel brands including Marriott, Courtyard, and Ritz-Carlton. Marriott reported revenues of \$20.75 billion in the 2018 fiscal year.

20. Upon information and belief, Marriott collects, stores, and maintains the PII of all guests who stay at Marriott properties.

21. As a condition of staying at one of its properties, Marriott requires that guests entrust it with their PII.

22. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Marriott assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

² <https://mysupport.marriott.com/>

23. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and the Class Members relied on Marriott to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

24. In Marriott's Global Privacy Statement dated May 18, 2018, Marriott represents that: "The Marriott Group, which includes Marriott International, Inc., Starwood Hotels & Resorts Worldwide, LLC ... and their affiliates, values you as our guest and recognizes that privacy is important to you." It explains that the Marriott Group collects data:

- through websites operated by us from which you are accessing this Privacy Statement, including Marriott.com and other websites owned or controlled by the Marriott Group (collectively, the "Websites")
- through the software applications made available by us for use on or through computers and mobile devices (the "Apps")
- through our social media pages that we control from which you are accessing this Privacy Statement (collectively, our "Social Media Pages")
- through HTML-formatted email messages that we send you that link to this Privacy Statement and through your communications with us
- when you visit or stay as a guest at one of our properties, or through other offline interactions.

25. The Privacy Statement defines "Collection of Personal Data" as follows: "Personal Data" are data that identify you as an individual or relate to an identifiable individual. At touchpoints throughout your guest journey, we collect Personal Data in accordance with law, such as:

- Name
- Gender
- Postal address
- Telephone number
- Email address
- Credit and debit card number or other payment data
- Financial information in limited circumstances
- Language preference
- Date and place of birth
- Nationality, passport, visa or other government-issued identification data
- Important dates, such as birthdays, anniversaries and special occasions •
- Membership or loyalty program data (including co-branded payment cards, travel partner program affiliations)
- Employer details
- Travel itinerary, tour group or activity data

26. Marriott further represents that: “We seek to use reasonable organizational, technical and administrative measures to protect Personal Data.”

27. Knowing the significant value and sensitive nature of the information it collects, Marriott’s current privacy policy represents that Marriott uses “reasonable physical, electronic, and administrative safeguards to protect your Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the nature of the Personal Data and the risks involved in processing that information.”³

³ Marriott U.S. Privacy Shield Guest Privacy Policy (updated May 24, 2019), *available at*:

28. Despite collecting and holding “Personal Data” for millions of individuals worldwide, Marriott failed to adopt reasonable data security measures to prevent and detect unauthorized access to their highly-sensitive databases. Marriott had the resources to prevent a breach and has made significant expenditures to market their hotels and hospitality services, but neglected to adequately invest in data security, despite being engaged in litigation regarding one of the largest data breaches in history.

C. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

29. The types of information compromised in the Data Breach are highly valuable to identity thieves. The names, email addresses, recovery email accounts, telephone numbers, payment card information, passport information, and other valuable PII can all be used to gain access to a variety of existing accounts and websites.

30. Identity thieves can also use the PII to harm Plaintiff and Class Members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver’s licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit

<https://www.marriott.com/about/global-privacy.mi> (last accessed March 31, 2020).

reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.⁴

31. To put it into context, the 2013 Norton Report, based on one of the largest consumer cybercrime studies ever conducted, estimated that the global price tag of cybercrime was around \$113 billion at that time, with the average cost per victim being \$298 dollars.

32. The problems associated with identity theft are exacerbated by the fact that many identity thieves will wait years before attempting to use the PII they have obtained. Indeed, in order to protect themselves, Class members will need to remain vigilant against unauthorized data use for years and decades to come.

33. Once stolen, PII can be used in a number of different ways. One of the most common is that it is offered for sale on the “dark web,” a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users’ identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and PII.⁵ Websites appear and disappear quickly, making it a very dynamic environment.

34. Once someone buys PII, it is then used to gain access to different areas of the victim’s digital life, including bank accounts, social media, and credit card details. During that

⁴ The President’s Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), <https://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf>

⁵ Brian Hamrick, *The dark web: A trip into the underbelly of the internet*, WLWT News (Feb. 9, 2017 8:51 PM), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419>.

process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

D. Marriott Failed to Comply With FTC Requirements

35. Federal and State governments have likewise established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁶

36. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.⁷ The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

37. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex

⁶ Federal Trade Commission, *Start With Security*, available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>

⁷ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>

passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.⁸

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

39. Marriott was at all times fully aware of its obligation to protect the personal and financial data of its guests and customers. Marriott was also aware of the significant repercussions if it failed to do so.

40. Marriott’s failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

E. The Marriott Data Breach Caused Harm and Will Result in Additional Fraud

41. The ramifications of Marriott’s failure to keep Plaintiff’s and Class members’ data secure are severe.

42. Consumer victims of data breaches are much more likely to become victim of identity fraud. This conclusion is based on an analysis of four years of data that correlated each year’s data breach victims with those who also reported being victims of identity fraud.⁹

⁸ FTC, *Start With Security*, *supra* note 5.

⁹ 2014 LexisNexis True Cost of Fraud Study, <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>.

43. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁰ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.”¹¹

44. PII is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, “they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.”¹²

45. Identity thieves can use personal information, such as that of Plaintiff and Class Members, which Marriott failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver’s license or identification card in the victim’s name but with another’s picture; using the victim’s information to obtain government benefits; or filing a fraudulent tax return using the victim’s information to obtain a fraudulent refund.

46. Javelin Strategy and Research reports that identity thieves have stolen \$112 billion in the past six years.¹³

47. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of

¹⁰ 17 C.F.R § 248.201 (2013).

¹¹ *Id.*

¹² Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>.

¹³ <https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point>

Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.¹⁴

48. An independent financial services industry research study conducted for BillGuard—a private enterprise that automates the consumer task of finding unauthorized transactions that might otherwise go undetected—calculated the average per-consumer cost of all unauthorized transactions at roughly US \$215 per cardholder incurring these charges,¹⁵ some portion of which could go undetected and thus must be paid entirely out-of-pocket by consumer victims of account or identity misuse.

49. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁶

50. Thus, Plaintiff and Class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

¹⁴ Victims of Identity Theft, 2014 (Sept. 2015) available at: <http://www.bjs.gov/content/pub/pdf/vit14.pdf>.

¹⁵ Hadley Malcom, *Consumers rack up \$14.3 billion in gray charges, research study commissioned for Billguard by Aite Research, USA Today* (July 25, 2013), available at: <https://www.usatoday.com/story/money/personalfinance/2013/07/25/consumers-unwanted-charges-in-billions/2568645/>.

¹⁶ GAO, Report to Congressional Requesters, at 29 (June 2007), <http://www.gao.gov/new.items/d07737.pdf>

F. Plaintiff and Class Members Suffered Damages

51. The PII of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by Marriott. Marriott did not obtain Plaintiff's and Class members' consent to disclose their PII to any other person as required by applicable law and industry standards.

52. The Data Breach was a direct and proximate result of Marriott's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriott's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

53. Marriott had the resources to prevent a breach. Marriott made significant expenditures to market its hotels and hospitality services, but neglected to adequately invest in data security, despite the growing number of data intrusions and several years of well-publicized data breaches, including its own massive breach a little over a year ago.

54. Had Marriott remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Marriott would have prevented intrusion into its information storage and security systems and, ultimately, the theft of its customers' confidential PII.

55. As a direct and proximate result of Marriott's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as

work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

56. Marriott’s wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff’s and Class members’ PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

- a. theft of their personal and financial information;
- b. the imminent and certainly impending injury flowing from potential fraud and identity theft;
- c. the untimely and inadequate notification of the Data Breach;
- d. the improper disclosure of their PII;
- e. loss of privacy;
- f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
- g. ascertainable losses in the form of deprivation of the value of their PII, for which there is a well-established national and international market;
- h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach.

57. While Plaintiff’ and Class members’ PII have been compromised, Marriott continues to hold consumers’ PII, including Plaintiff and Class members. Particularly because

Marriott has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PII is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

G. Marriott's Offer of Credit Monitoring is Inadequate

58. At present, Marriott has offered one year of free enrollment in Experian's IdentityWorks, a credit monitoring service.

59. As previously alleged, consumers' PII may exist on the Dark Web for months, or even years, before it is used for ill gains and actions. With only one year of monitoring, and no form of insurance or other protection, Plaintiff and Class Members remain unprotected from the real and long-term threats against their PII.

60. Therefore, the "monitoring" services are inadequate, and Plaintiff and Class Members have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

61. Marriott's response to the Data Breach, and the services it offered to consumers to address the breach, are insufficient, resulting in consumers spending a significant amount of time taking measures to protect themselves. Thus, Marriott cannot be heard to complain about customers taking its advice and suggestions for how to respond in the face of this latest Data Breach to be suffered by Marriott customers.

CLASS ACTION ALLEGATIONS

62. Pursuant to Fed. R. Civ. P. 23(b)(2), (b)(3) and (c)(4), Plaintiff, individually and on behalf of all others similarly situated, brings this lawsuit on behalf of themselves and as a class action on behalf of the following class:

All persons in the United States who provided PII to Marriott and whose PII was accessed, compromised, or stolen from Marriott in the Data Breach announced on March 31, 2020.

63. Excluded from the Class are Defendant and any entities in which any Defendant or its subsidiaries or affiliates have a controlling interest, and Defendant's officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, members of the judge's staff, and any member of the judge's immediate family.

64. **Numerosity:** The members of each Class are so numerous that joinder of all members of any Class would be impracticable. The Class consists of approximately 5.2 million Marriott customers. The names and addresses of Class members are identifiable through documents maintained by Defendant.

65. **Commonality and Predominance:** This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

- i. Whether Defendant represented to the Class that it would safeguard Class members' PII;
- ii. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- iii. Whether Defendant breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- iv. Whether Class members' PII was accessed, compromised, or stolen in the Data Breach;

- v. Whether Defendant knew or should have known that its computer data systems were vulnerable to attack;
- vi. Whether Defendant knew about the Data Breach before it was announced to the public and Defendant failed to timely notify the public of the Data Breach;
- vii. Whether Defendant's conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*,
- viii. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and
- ix. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

66. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

67. **Typicality:** Plaintiff's claims are typical of the claims of the other members of their respective classes because, among other things, Plaintiff and the other Class members were injured through the substantially uniform misconduct by Defendant. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. Plaintiff's claims and those of other Class members arise from the same operative facts and are based on the same legal theories.

68. **Adequacy of Representation:** Plaintiff is an adequate representative of the class because her interests do not conflict with the interests of the other Class members she seeks to represent; she has retained counsel competent and experienced in complex class action litigation and Plaintiff will prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiff and her counsel.

69. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the other members of their respective classes are relatively small compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendant, making it impracticable for Class members to individually seek redress for Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments, and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

70. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

71. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Class members' PII was accessed, compromised, or stolen in the Data Breach;

- b. Whether (and when) Defendant knew about any security vulnerabilities that led to the Data Breach before it was announced to the public and whether Defendant failed to timely notify the public of those vulnerabilities and the Data Breach;
- c. Whether Defendant's representations that it would secure and protect the PII of Plaintiff and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Defendant's services;
- d. Whether Defendant misrepresented the safety of its many systems and services, specifically the security thereof, and its ability to safely store Plaintiff's and Class members' PII;
- e. Whether Defendant concealed crucial information about its inadequate data security measures from Plaintiff and the Class;
- f. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- g. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent the loss or misuse of that information;
- h. Whether Defendant failed to "implement and maintain reasonable security procedures and practices" for Plaintiff's and Class members' PII in violation of Section 5 of the FTC Act;
- i. Whether Defendant failed to provide timely notice of the Data Breach in violation of state consumer protection laws, including Md. Code Com. Law § 14-3501, *et seq.*;

- j. Whether Defendant owed a duty to Plaintiff and the Class to safeguard their PII and to implement adequate data security measures;
- k. Whether Defendant breached that duty;
- l. Whether such representations were false with regard to storing and safeguarding Plaintiff's and Class members' PII; and
- m. Whether such representations were material with regard to storing and safeguarding Class members' PII.

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief
Negligence

72. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 71 as though fully stated herein.

73. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Marriott's security systems to ensure that Plaintiff's and class members' PII in Marriott's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

74. Defendant knew that the PII belonging to Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the PII of Plaintiff and the Class was wrongfully

disclosed, that disclosure was not fixed, or Plaintiff and the Class were not told about the disclosure in a timely manner.

75. By being entrusted by Plaintiff and the Class to safeguard their PII, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class signed up for and paid for Defendant's services and agreed to provide their PII with the understanding that Defendant would take appropriate measures to protect it, and would inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class. Defendant did not.

76. Marriott had a common law duty to prevent foreseeable harm to its customers. This duty existed because Plaintiff and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, Marriott knew that it was more likely than not Plaintiff and other class members would be harmed.

77. Defendant is morally culpable, given the prominence of security breaches in the hospitality industry and its own recent massive breach which demonstrated Defendant's wholly inadequate cyber security measures and safeguards.

78. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite repeated failures and intrusions, and allowing unauthorized access to Plaintiff's and the other Class member's PII.

79. Marriott breached the duties it owed to Plaintiff and class members described above and thus was negligent. Marriott breached these duties by, among other things, failing to: (a)

exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose in a timely fashion that Plaintiff's and the class members' PII in Marriott's possession had been or was reasonably believed to have been, stolen or compromised.

80. Defendant's failure to comply with industry and federal regulations further evidences Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII.

81. Defendant's breaches of these duties were not merely isolated incidents or small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term company-wide refusal by Defendant to acknowledge and correct serious and ongoing data security problems.

82. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII of Plaintiff and the Class and all resulting damages.

83. Marriott also had a duty to safeguard the PII of Plaintiff and class members and to promptly notify them of a breach because of laws and regulations that require Marriott to reasonably safeguard PII, as detailed herein.

84. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and class members could take appropriate measures to freeze or lock their credit profiles, cancel current passports and obtain new passports, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their

banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Marriott's misconduct.

85. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other class members' PII. Defendant knew its systems and technologies for processing and securing the PII of Plaintiff and the Class had numerous security vulnerabilities.

86. As a result of this misconduct by Defendant, the PII of Plaintiff and the Class were compromised, placing them at a greater risk of identity theft and subjecting them to identity theft, and their PII was disclosed to third parties without their consent. Plaintiff and Class members also suffered diminution in value of their PII in that it is now easily available to hackers on the dark web. Plaintiff and the Class have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Second Claim for Relief
Negligence Per Se

87. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 71 as though fully stated herein.

88. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Marriott, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Marriott's duty in this regard.

89. Marriott violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Marriott's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach at a hospitality chain as large as Marriott, including, specifically, the immense damages that would result to Plaintiff and Class Members.

90. Marriott's violation of Section 5 of the FTC Act constitutes negligence *per se*.

91. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

92. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

93. As a direct and proximate result of Marriott's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

94. Additionally, as a direct and proximate result of Marriott's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their

PII, which remain in Marriott's possession and is subject to further unauthorized disclosures so long as Marriott fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

Third Claim for Relief
Breach of Contract

95. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 71 as though fully stated herein.

96. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

97. Marriott's Privacy Statement is an agreement between Marriott and individuals who provided their PII to Marriott, including Plaintiff and Class Members

98. Marriott's Privacy Statement states that individuals are subject to its terms and conditions when they perform any of the following acts: (1) log onto Marriott's website; (2) use Marriott's software applications; (3) access Marriott's social media pages; (4) receive e-mail communications from Marriott that link to the Privacy Statement; and (5) "when you visit or stay as a guest at one of our properties, or through other offline interactions." Marriott's Privacy Statement provides that: "Collectively, we refer to the Websites, the Apps and our Social Media Pages, as the 'Online Services' and, together with offline channels, the 'Services.' ***By using the Services, you agree to the terms and conditions of this Privacy Statement.***" (emphasis added).

99. Likewise, the terms and conditions governing the Marriott Rewards Program state that: "By opening a Membership Rewards Program account ... You consent to the Company's processing of data that is personal to You, and disclosure of such data to third parties, in accordance with the Company's privacy statement."

100. Plaintiff and class members provided their PII to Marriott when they, among other things, used Marriott's services, enrolled in Marriott's Reward Program, purchased products and services from Marriott, and/or booked reservations at a Marriott Property via offline and online channels. Consequently, Plaintiff and Class Members who transacted with Marriott manifested their willingness to enter into a bargain with Marriott and intention to assent to the terms of the Privacy Statement by providing their PII to Marriott.

101. Conversely, Marriott, in collecting Plaintiff's and class members' PII, manifested its intent to adhere to its obligations under the Privacy Statement, including using "reasonable organizational, technical and administrative measures to protect [its customers'] Personal Data."

102. Plaintiff and class members on the one hand and Marriott on the other formed contracts when Plaintiff and class members provided PII to Marriott subject to their Privacy Statement.

103. Plaintiff and Class Members fully performed their obligations under the contracts with Marriott.

104. Marriott breached its agreements with Plaintiff and Class Members by failing to protect their PII. Specifically, Marriott (1) failed to use reasonable organizational, technical, procedural, and administrative measures to protect that information; and (2) disclosed that information to unauthorized third parties, in violation of their agreements.

105. As a direct and proximate result of these breaches of contract, Plaintiff and class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid.

Fourth Claim for Relief
Breach of Implied Contract

106. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 71 as though fully stated herein.

107. Plaintiff and Class Members also entered into an implied contract with Marriott when they obtained services from Marriott, or otherwise provided PII to Marriott.

108. As part of these transactions, Marriott agreed to safeguard and protect the PII of Plaintiff and Class Members and to timely and accurately notify them if their PII was breached or compromised.

109. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Marriott's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Marriott would use part of the monies paid to Marriott under the implied contracts to fund adequate and reasonable data security practices.

110. Plaintiff and Class Members would not have provided and entrusted their PII to Marriott or would have paid less for Marriott's services in the absence of the implied contract or implied terms between them and Marriott. The safeguarding of the PII of Plaintiff and Class Members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

111. Plaintiff and Class Members fully performed their obligations under the implied contracts with Marriott.

112. Marriott breached its implied contracts with Plaintiff and Class Members to protect their PII when it (1) failed to have security protocols and measures in place to protect that

information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their PII was compromised as a result of the data breach.

113. As a direct and proximate result of Marriott's breaches of implied contract, Plaintiff and Class Members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid

Fifth Claim for Relief
Breach of Confidence

114. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 71 as though fully stated herein.

115. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and Class Members provided to Defendant.

116. As alleged herein and above, Defendant's relationship with Plaintiff and Class Members was governed by expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

117. Plaintiff and Class Members provided their respective PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

118. Plaintiff and Class Members also provided their respective PII to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

119. Defendant voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

120. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' Customer Data was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

121. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

122. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

123. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew its computer systems and cyber security practices for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities because Defendant failed to observe industry standard information security practices.

124. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from identity theft; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting

agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy.

125. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

Sixth Claim for Relief
Violation of Maryland's Consumer Protection Act
Deceptive and Unfair Trade Practices
Title 13, Section 13-101, *et seq.*

126. Plaintiff repeats, realleges, and incorporates by reference the allegations contained in paragraphs 1 through 71 as though fully stated herein.

127. Plaintiff and Class members are consumers for the purposes of Maryland's Consumer Protection Act.

128. Defendant is merchant for the purposes of Maryland's Consumer Protection Act.

129. Defendant, by failing to inform consumers (including Plaintiff and the Class Members) of Defendant's insufficient cyber security practices, advertised, sold, serviced, and otherwise induced those consumers (including Plaintiff and Class Members) to purchase goods and services from Defendant.

130. By failing to inform consumers (including Plaintiff and the Class Members) of its deficient cyber security practices, Defendant falsely represented the security of its data and

information security practices to safeguard the PII Defendant collected from its guests (including Plaintiff and the Class Members).

131. Defendant's failures constitute false, misleading, and misrepresentations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff and Class Members) concerning the security of their networks and aggregation of PII.

132. In addition, the facts upon which consumers (including Plaintiff and Class Members) relied were material facts, the veracity of which were not true (e.g., protection of PII), and consumers (including Plaintiff and Class Members) relied on those false facts to their detriment.

133. Defendant employed these false representations to promote the sale of a consumer good or service, which Plaintiff and the Class Members purchased.

134. As a direct and proximate result of Defendant's actions, Plaintiff and Class Members have suffered and will continue to suffer injury, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully request this Court enter an Order:

- a. An Order certifying this case as a class action;
- b. An Order appointing Plaintiff as the class representative;
- c. An Order appointing undersigned counsel as class counsel;
- d. A mandatory injunction directing the Defendants to hereinafter adequately safeguard the PII of the Class by implementing improved security procedures and measures;
- e. An award of damages;

- f. An award of costs and expenses;
- g. An award of attorneys' fees; and
- h. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims so triable.

Dated: April 1, 2020

/s/ William H. Murphy III
William H. Murphy III, Esq.

MURPHY, FALCON & MURPHY, P.A.
William H. Murphy III, Esq. (Bar No. 30126)
hassan.murphy@murphyfalcon.com
One South Street, 30th Floor
Baltimore, MD 21202
Telephone: (410) 951-8744
Facsimile: (410) 539-6599

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
John A. Yanchunis (Pro Hac Vice Forthcoming)
jyanchunis@ForThePeople.com
Jean S. Martin (Pro Hac Vice Forthcoming)
jeanmartin@ForThePeople.com
Ryan J. McGee (Pro Hac Vice Forthcoming)
rmcgee@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813/223-5505
813/223-5402 (fax)

Attorney for Plaintiff and the Class